SDD:UAD
F.#2014R00043

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

17M82

----------X

UNITED STATES OF AMERICA

- against -

ANTON BOGDANOV,
also known as "Kusok,"

Defendant.

----------X

TO BE FILED UNDER SEAL

AFFIDAVIT IN SUPPORT OF
ARREST WARRANT
(18 U.S.C. §§ 1030(a)(2)(B) & (C))

EASTERN DISTRICT OF NEW YORK, SS:

MATTHEW ALEX, being duly sworn, deposes and states that he is a Special Agent with the Federal Bureau of Investigation ("FBI") duly appointed according to law and acting as such.

Count One: Unauthorized Computer Intrusions

In or about and between June 2014 and November 2016, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant ANTON BOGDANOV, also known as "Kusok," together with others, did intentionally access a computer without authorization and exceeded authorized access, and thereby obtained information from any department and agency of the United States, to wit: tax transcripts from the United States Department of the Treasury, the value of which exceeded $5,000.

(Title 18, United States Code, Sections 1030(a)(2)(B), 2 and 3551 et seq.)

Count Two: Unauthorized Computer Intrusions

In or about and between April 2016 and December 2016, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant ANTON BOGDANOV, also known as "Kusok," together with others, did intentionally access a computer without authorization and exceeded authorized access, and thereby obtained information from a protected computer, to wit: tax filings from tax preparation firms, for the purposes of commercial advantage and private financial gain.

(Title 18, United States Code, Sections 1030(a)(2)(B), 2 and 3551 et seq.)

The source of your deponent's information and the grounds for his belief are as follows:

1. I have been a Special Agent with the Federal Bureau of Investigation ("FBI") since 2011. I am responsible for conducting and assisting in investigations into the activities of individuals and criminal groups responsible for crimes related to, among others, computer-related crimes, including access device fraud. These investigations are conducted both in an undercover and overt capacity. I have participated in investigations involving search warrants and arrest warrants. As a result of my training and experience, I am familiar with the techniques and methods of operation used by individuals involved in criminal activity to conceal their activities from detection by law enforcement authorities.

2. The facts in this affidavit come from my personal observations, my training and experience, information obtained from other agents, cooperating witnesses and a review of records and documents. Because the purpose of this affidavit is limited to demonstrating probable cause for the requested warrant, it does not set forth all of my

knowledge about this matter. In addition, when I rely on statements made by others, such statements are set forth only in part and in substance unless otherwise indicated.

A. The Criminal Scheme

3. In February 2014, the FBI identified and arrested an individual for access device fraud. Following the arrest, the individual became a cooperating witness ("CW-1") for the government.[1] Following his arrest, CW-1 continued to receive and carry out instructions from individuals with whom he worked.

4. Pursuant to information provided by CW-1, the FBI began investigating a co-conspirator ("CW-2"). In February 2016, the FBI arrested CW-2. CW-2 also began cooperating with the government's investigation.[2]

5. Through interviews, a review of chat logs and other investigation, the FBI learned that CW-1 provided, among other things, "cashing" services for CW-2 since in or around March 2013. Specifically, CW-2 would fraudulently obtain prepaid debit cards using stolen personally identifiable information ("PII") and load the cards with funds obtained through a variety of criminal schemes, including income tax refund fraud and ransomware. CW-1 was responsible for "cashing out" the prepaid debit cards and forwarding the funds (less CW-1's fee) at the direction of CW-2.[3]

---

[1] CW-1 has since pleaded guilty to, among other crimes, access device fraud and aggravated identity theft. The cooperating witnesses referred to herein as CW-1 and CW-2 are cooperating in the hopes of receiving leniency at sentencing, and their information has proven reliable and has been corroborated.

[2] CW-2 has since pleaded guilty to, among other crimes, access device fraud, theft of government property and aggravated identity theft.

[3] "Cashing out" means withdrawing the funds from the debit cards. That can be done through a variety of mechanisms, including withdrawing cash from banks or ATMs and

6. CW-2 frequently provided his services (i.e., obtaining, loading and cashing out fraudulently obtained prepaid debit cards) to others whom he met in various online criminal forums.

7. On or about June 25, 2014, an individual with the online moniker "Kusok" sent a private message to CW-2 asking if CW-2 could provide prepaid cards that could receive direct deposits from the Internal Revenue Service ("IRS").[4] In this message, "Kusok" provided his jabber account[5] to CW-2 for further communication.

8. On or about July 25, 2014, "Kusok" told CW-2, in sum and substance, that he had the ability to file for hundreds of thousands of dollars in business tax refunds using what CW-2 understood to be fraudulently obtained information. Kusok sought prepaid debit cards from CW-2. It was CW-2's understanding that "Kusok" provided the prepaid debit card information[6] to the IRS in the fraudulent tax filings as the account to which the return should be deposited.

9. On July 27, 2014, "Kusok" asked CW-2 to provide twenty-one prepaid debit cards. In response, CW-2 electronically sent "Kusok" ten fraudulently obtained prepaid

---

electronically transferring the funds from the debit cards to other accounts.

[4] The FBI was able to recover chats between CW-2 and "Kusok" from CW-2's computer following CW-2 arrest and also preserved chats between CW-2 and "Kusok" post-dating CW-2's arrest.

[5] Jabber is a chat protocol that allows for private hosting of servers, in contrast to corporate hosting by companies such as Yahoo! and Google. Moreover, Jabber allows for encryption, which permits users to encrypt their communications and keep their communications private, even from the administrators of the servers through which their communications were routed. Jabber is thus known as a secure chat protocol which can be used by criminals to evade detection by law enforcement.

[6] Certain prepaid debit cards have routing numbers and account number and can receive deposits in the same fashion as bank accounts.

debit cards that day and an additional eleven the next.[7] CW-2 also told "Kusok" that he could supply additional prepaid debit cards if "Kusok" provided personally identifiable information ("PII") of individuals with which to apply for prepaid debit cards.

10. On or about July 31, 2014, "Kusok" informed CW-2 that there was money on some of the prepaid debit cards that CW-2 had previously provided. CW-2 informed "Kusok" that those prepaid debit cards had in fact already been cashed. "Kusok" provided a Webmoney[8] address to which CW-2 was to send "Kusok's" share of the proceeds, which was fifty-five percent.

11. It was CW-2's understanding that "Kusok" prepared his fraudulent tax filings using PII and banking, earnings and other information from the tax transcripts of tax filers from prior years.[9] As part of their working arrangement, CW-2 asked "Kusok" to teach him how to apply for tax refunds. On or about August 2, 2014, "Kusok" electronically sent CW-2 instructions on how to unlawfully obtain tax transcripts from the IRS through its website.

12. On or about August 20, 2014, "Kusok" electronically sent CW-2 PII for ten individuals and requested that CW-2 apply for prepaid debit cards that could accept government payment, and specifically mentioned Akimbo Card. Based on my training and

---

[7] CW-2 did not send the physical cards, but provided "Kusok" electronically with the information from the cards for "Kusok" to use with his tax filings.

[8] Webmoney is a virtual currency exchange based in Russia, which uses WebMoney units (WM) as currency.

[9] A tax transcript is a copy of a tax filer's prior tax return filing. The IRS keeps records of tax transcripts, and obtaining an individual's tax transcript would provide a criminal sufficient information with which to file a fraudulent return in the victim's name.

experience, cards that can accept government payment refers to prepaid debit cards that have associated routing and account numbers, like a bank account.

13. On or about September 16, 2014, "Kusok" sent additional PII to CW-2 and said he could provide PII for 10-15 individuals per week.

14. Thereafter, until approximately January 2016, "Kusok" continued to send PII to CW-2, and CW-2 used the PII to open prepaid debit cards for use by "Kusok" in the tax refund fraud scheme. After CW-2 obtained the prepaid cards, he would electronically send the card information to "Kusok" for use in fraudulent tax filings. Approved tax refunds would then be deposited onto the prepaid debit cards, whereupon CW-2 would instruct CW-1 to cash out the cards.

15. Between approximately September 2014 and January 2016, according to CW-2, "Kusok" sent PII for more than 350 individuals, which PII CW-2 used to obtain prepaid debit cards. Of those, based on the addresses listed, at least ten of the individuals resided in the Eastern District of New York. Analysis of a file found on CW-2's computer confirms CW-2's account. Analysis of records found on CW-2's computer also confirms that CW-2 processed at least $445,000 in fraudulent tax filings for "Kusok" in 2015. In subsequent chats between CW-2 and "Kusok," "Kusok" confirmed that his scheme involved using unlawfully obtained tax transcripts from the IRS website.

16. On or about April 15, 2016, "Kusok" told CW-2 in a consensually monitored jabber chat that he had purchased remote desktop protocol ("RDP") access to the computer networks of numerous tax preparation firms. "Kusok" stated that he electronically changed the tax filings of the firm's clients so that the account and routing numbers listed in

filings (and to which refunds were to be paid) were those of his prepaid debit cards. "Kusok" stated he paid approximately $3,000 to $4,000 for each set of RDP access credentials he obtained. "Kusok" did not specify from whom he had obtained the RDP credentials, but based on my training and experience, I am aware that stolen credentials such as RDP credentials can be purchased via online criminal forums.

17. Based on my training and experience, I am aware that RDP credentials allow a user to log into a computer network from a remote location. If a criminal such as "Kusok" connects remotely to a tax preparation firm's computer system using stolen credentials of an authorized user, he can alter the tax returns of the firm's clients. Specifically, RDP access would allow "Kusok" to change the account and routing numbers of the accounts to which the tax refunds are to be deposited and substitute that with account information from the prepaid debit cards provided by CW-2. "Kusok" told CW-2 that while he had access to a firm's network, he also typically downloaded the preparation firm's client data for future use.

18. On or about April 21, 2016, "Kusok" told CW-2 in a consensually monitored jabber chat he had three databases containing tax information for approximately 1,000 individuals, which he said he obtained from tax preparation companies through RDP access. "Kusok" explained that he was planning to purchase RDP access to another tax preparation firm for $2,700. "Kusok" further stated that he believed he would then have access to tax information for an additional 3,000 individuals.

19. On or about June 10, 2016, "Kusok" told CW-2 in a consensually monitored jabber chat that he had a 90% success rate in that year's tax season, and that he used RDP access to change the direct deposit information on the tax filings, which amounted to

more than $2,000,000 in refunds. However, "Kusok" reported that the refunds were never released by the IRS onto the prepaid debit card accounts. "Kusok" believed the tax refunds were blocked by the IRS because the name on the prepaid debit cards did not match the name on the tax return filing.

20. By tracking the prepaid debit cards fraudulently obtained by CW-2 (and later cashed out by CW-1), the FBI, in conjunction with the IRS, was able to identify tax filings affected by Kusok's criminal scheme.[10] The investigation revealed six accounting firms in the United States that prepared tax returns in which CW-2's prepaid debit cards were listed as the direct deposit account for the return. Interviews of five of these firms confirm that they were the subject of an RDP breach and that the firms did not intentionally submit those prepaid debit card account numbers with the filings. One of the firms is located in the Eastern District of New York.

21. On or about November 11, 2016, "Kusok" sent to CW-2 PII for an individual that the FBI has confirmed is a United States citizen. "Kusok" stated that he obtained the PII by obtaining the tax transcript for this individual from the IRS website. "Kusok" wanted CW-2 to obtain a prepaid debit card using the PII.

22. On or about December 31, 2016, "Kusok" sent CW-2 a private message, which message contained PII for approximately thirty individuals. Investigation revealed that most of these individuals reside in Idaho. Together with the IRS, the FBI identified an

---

[10] CW-1 was cooperating with the government's investigation for the entire time period during which CW-2 and Kusok worked together and was responsible for "cashing out" the prepaid debit cards. As such, the FBI was able track the prepaid cards that CW-1 cashed at CW-2's direction.

accounting and tax preparation firm as the source of the PII. An interview with the firm revealed that it was recently the victim of an unauthorized RDP into its network. Investigation further revealed that in and around December 15, 2016, someone had created folders in one of the firm's network user accounts and placed more than five hundred copies of tax returns of the firm's clients in these folders. The firm confirmed that these folders had not been created by any of its employees. Additionally, these folders had been compressed into .rar files.[11] Based on my training and experience, I believe that the compression of these tax returns into .rar files is indicative of that data having been exfiltrated, since compressing data renders it easier to transmit via the internet.

B. "Kusok" is Anton Bogdanov

23. Investigation has revealed that "Kusok" is an individual named "Anton Bogdanov."

24. Investigation also revealed that the user "Kusok" on the online criminal forum Verified used the ICQ number 275232. User "Kusok" on online criminal websites Cardingworld.cc and Carder.su also used the ICQ number 275232. On Cardingworld.cc, "Kusok" registered using the email address durmalin88@mail.ru (the "durmalin88 email").

25. The durmalin88 email is also the registrant for the domain ba-bola.com and multiple other domains. The registrant's name on these domains is "Anton Bogdanov." The registrant's telephone number is a number ending in 1059 (the "1059 number"), which resolves to Moscow, Russia.

---

[11] RAR files are data containers, storing one or more files in compressed form. Compressing data makes the data easier to transfer.

26. The durmalin88 email is also the recovery email for an Apple account, number 10031796987. Anton Bogdanov is listed as the name on the account, and the primary email address for the Apple account is babolaru@gmail.com.

27. Records received from Google reveal that both babolaru@gmail.com and another email account b0gdap777@gmail.com list the durmalin88 email as the recovery email for each. The name on these gmail accounts is Cyrillic for Anton Bogdanov. These records also reveal that these gmail accounts are associated with the 1059 number.

28. Investigation also revealed a mail.ru domain that contains a user profile page for the durmalin88 email account. The name on the profile page is "Anton Bogdanov" (translated from Russian) and contains approximately 20 user-uploaded photographs.[12]

29. A search on Russian social networking site Vkontakte (commonly referred to as "VK") for user "Anton Bogdanov" revealed an account containing over two hundred user-uploaded photographs, which included the twenty photographs found in the mail.ru domain associated with the durmalin88 email. Photos posted on this account repeatedly show one particular male, who I believe to be BOGDANOV.

WHEREFORE your deponent respectfully requests that an arrest warrant issue for the defendant ANTON BOGDANOV, also known as "Kusok," so that he may be dealt with according to law. I further request that the Court order that this application, including the affidavit and arrest warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation. Disclosure of this application and these orders

---

[12] This profile page is linked to the durmalin88 email, which is also hosted by mail.ru and appears to function like a social networking page.

would seriously jeopardize the ongoing investigation, as such a disclosure would give the targets of the investigation an opportunity to destroy evidence, harm or threaten victims or other witnesses, change patterns of behavior, notify confederates and flee from or evade prosecution.

Matthew Alex
Special Agent, FBI

Sworn to before me this
30th
S/TISCIONE

THE HONORABLE STEVEN L. TISCIONE
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK